Campanha de Conscientização Cibernética

REDES SOCIAIS

Para usar as redes sociais **com segurança** é importante tomar cuidados para não se **expor** em excesso ou cair em golpes.

Veja aqui como se proteger.

CUIDADOS ESSENCIAIS NAS REDES SOCIAIS

PENSE BEM ANTES DE POSTAR

Nas redes sociais as informações se **propagam** rapidamente e, depois que algo é divulgado, dificilmente pode ser apagado ou controlado. Alguém pode já ter copiado e passado adiante.

- » Lembre-se: **uma vez postado, sempre postado**
- » Considere que você está em um local público
  - tudo que você posta pode ser visto por alguém, tanto agora como no futuro

SEJA SELETIVO AO ACEITAR SEGUIDORES

Quanto maior sua rede, maior a **exposição** de seus dados, postagens e lista de contatos. Isso aumenta o risco de **abuso** dessas informações. Aceitar qualquer contato facilita a ação de pessoas mal-intencionadas.

» Configure sua conta como **privada**, quando possível

» Verifique a **identidade** da pessoa antes de aceitá-la em sua rede

- bloqueie contas falsas

LIMITE O COMPARTILHAMENTO DE INFORMAÇÕES DO SEU PERFIL

Algumas redes sociais não permitem contas privadas e dão **acesso público** às informações do seu perfil. Para controlar como tais informações são compartilhadas, há ajustes que você pode fazer.

» Evite compartilhar publicamente **informações pessoais**
  • por exemplo, número de telefone

» Ajuste o público-alvo das informações que compartilha

CONTROLE QUEM PODE VER SUAS POSTAGENS

Sua rede pode ser variada, com contatos próximos, outros nem tanto. Você pode escolher **compartilhar** postagens diferentes com pessoas diferentes para **minimizar** sua exposição.

» **Selecione** o público-alvo de suas postagens
  - crie listas **personalizadas** de contatos, quando a plataforma permitir

PROTEJA O ACESSO À SUA CONTA

Contas de redes sociais são valiosas para atacantes, que tentam invadi-las e usá-las para espalhar *malware* e aplicar golpes na **rede de contatos**. Eles se aproveitam da confiança entre os usuários e da velocidade com que as informações se propagam.

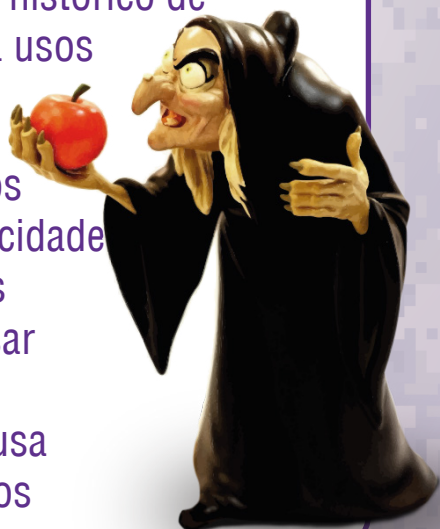
- Crie senhas fortes e ative a verificação em duas etapas
- Ative **alertas** e notificações de tentativas de acesso em suas contas
  - redobre a atenção com contas que dão acesso a outras (*login* social)
- Se alguma conta sua for **invadida**:
  - troque a senha
  - siga os procedimentos para recuperação do acesso, se necessário

Veja mais dicas na Cartilha

AUTENTICAÇÃO

Aplicativos de terceiros, como jogos, testes de personalidade e edição de imagens, podem **capturar** suas informações pessoais, fotos, histórico de navegação e lista de contatos para usos diversos e **abusivos**.

» Pense bem antes de dar acessos
  - **leia os termos** de uso e privacidade

» Verifique **periodicamente** quais aplicativos e *sites* podem acessar suas contas
  - revogue os acessos que não usa mais ou possam ser maliciosos

AJUSTE AS CONFIGURAÇÕES DE SEGURANÇA E PRIVACIDADE

As configurações de segurança e privacidade das plataformas ajudam a definir **quais** informações são compartilhadas sobre você e **como** suas informações são tratadas.

» Configure suas redes sociais de forma que se sinta confortável
  - procure o **equilíbrio** entre exposição, segurança e privacidade

NÃO ACREDITE EM TUDO O QUE VÊ NAS REDES SOCIAIS

Nas redes sociais circulam informações de qualquer tipo e origem, inclusive falsas e maliciosas. **Acreditar cegamente** em tudo que recebe ou acessa facilita a **ação de golpistas**.

- » Busque informações em outras fontes
- » Tenha cuidado ao clicar em *links*
  - mesmo vindo de pessoas conhecidas
  - atenção especial a **anúncios patrocinados**, pois podem ser maliciosos
- » Cuidado com mensagens que recebe via *chats*

DENUNCIE CONTEÚDOS MALICIOSOS E PERFIS FALSOS

Por meio de denúncias, as plataformas conseguem identificar contas falsas e os conteúdos indevidos e maliciosos.

» Use as opções de **denunciar**
» **Bloqueie** os conteúdos e perfis que estiverem incomodando
» Avise seus contatos se detectar contas falsas se passando por eles

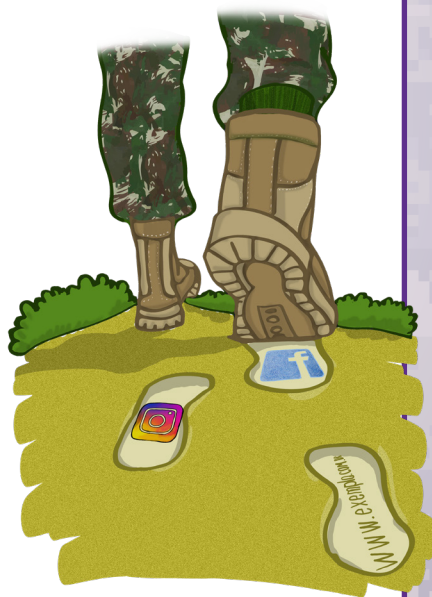
CUIDADOS COM SUA REPUTAÇÃO ONLINE

PROTEJA SEU FUTURO PROFISSIONAL

O conjunto de informações existentes sobre você nas redes sociais pode ser usado por empresas e recrutadores para **conhecê-lo melhor**.

» Avalie se suas postagens podem afetar negativamente sua imagem

» Separe seus contatos em redes ou listas **específicas**
- poste de acordo com o público a que se destina

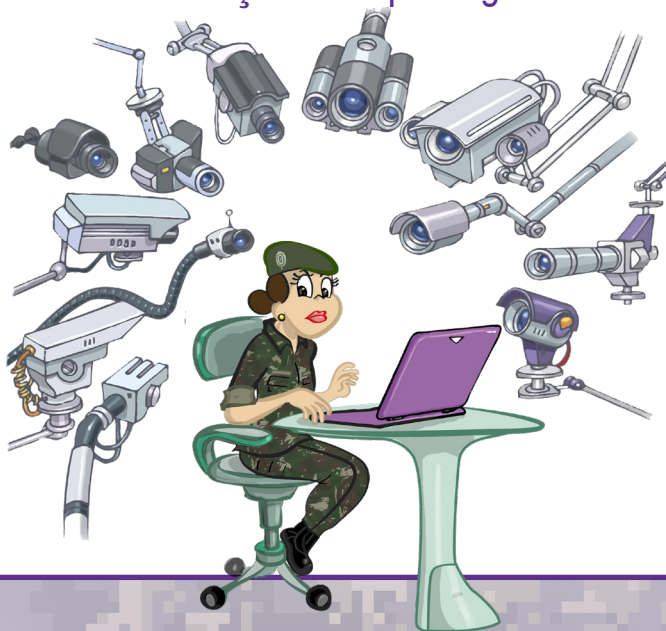
» Respeite a política de uso das redes sociais. Fique atento ao previsto no **Art. 11** da Portaria-EME/C Ex Nº 453, de 19 de julho de 2021

CUIDADO COM O QUE CURTE OU COMPARTILHA

Suas interações sociais, como curtidas e compartilhamentos, dizem muito sobre você, pois demonstram seu apoio àquele conteúdo. Se o conteúdo for indevido, isso pode gerar consequências, inclusive judiciais.

» Não curta nem compartilhe conteúdos que envolvam:
  - violência
  - calúnia e difamação
  - discriminação

SAIBA O QUE POSTAM SOBRE VOCÊ

Outros usuários podem marcar ou mencionar você em postagens e **expor a sua privacidade**. Apesar de não ser possível impedir, você pode **escolher** não incluir tais postagens em seu perfil.

» Configure para que possa **analisar** postagens em que for marcado
  - se não se sentir confortável, peça para a pessoa excluir a marcação ou a postagem

RESPEITE A PRIVACIDADE ALHEIA

Algumas pessoas não gostam de ter a **privacidade exposta** nas redes sociais. Pense como você se sentiria se fizessem isso com você.

» Evite falar sobre as ações, hábitos e rotina de outras pessoas
  - pense como elas se sentiriam se aquilo se tornasse público

» Peça autorização antes de:
  - postar imagens em que outras pessoas apareçam
  - compartilhar postagens de outras pessoas

SAIBA MAIS
Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais fascículos da Campanha de Conscientização Cibernética no site EB.MIL.BR

EXÉRCITO BRASILEIRO

Novos Desafios, Mesmos Valores

Produção: